PCT WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 7 : G06F 1/00 — A1

(11) International Publication Number: WO 00/19296

(43) International Publication Date: 6 April 2000 (06.04.00)

(21) International Application Number: PCT/CA99/00891

(22) International Filing Date: 24 September 1999 (24.09.99)

(30) Priority Data:
2,246,006 25 September 1998 (25.09.98) CA

(71) Applicant: SILANIS TECHNOLOGY INC. [CA/CA]; Suite 305, 3333, Côte Vertu, St. Laurent, Québec H4R 2N1 (CA).

(72) Inventors: SILVESTER, Joseph; 282, place des Cèdres, Dollard–des–Ormeaux, Québec H9G 1W1 (CA). MILCZAREK, Ed; 5135 des Cajeux, Pierrefonds, Québec H9J 3C4 (CA). PETROGIANNIS, Tommy; 4560 Cumberland Avenue, Montréal, Québec H4B 2L4 (CA).

(74) Agent: ROBIC; 55, St. Jacques, Montréal, Québec H2Y 3X2 (CA).

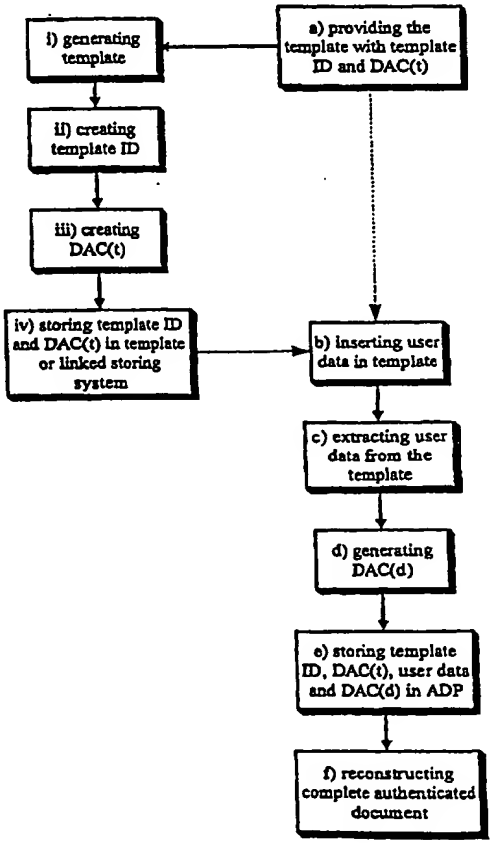
(81) Designated States: AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CU, CZ, DE, DK, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, UA, UG, UZ, VN, YU, ZW, ARIPO patent (GH, GM, KE, LS, MW, SD, SL, SZ, TZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

Published
With international search report.

(54) Title: METHOD FOR THE SEPARATE AUTHENTICATION OF A TEMPLATE AND USER DATA

(57) Abstract

A method for the separate authentication of a template and of data inserted therein. A template is provided with a template ID and a template Data Authentication Code (DAC(t)). User data is inserted in the template, and then extracted to be handled separately. A DAC(d) is generated on the user data by itself, and stored in an Approval Data packet with the template ID, DAC(t) and the user data. The complete document with the template and the user data can later be reconstructed. The method may be useful for many industries that rely on templates as a means for collecting data.



FOR THE PURPOSES OF INFORMATION ONLY

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

AL	Albania	ES	Spain	LS	Lesotho	SI	Slovenia
AM	Armenia	FI	Finland	LT	Lithuania	SK	Slovakia
AT	Austria	FR	France	LU	Luxembourg	SN	Senegal
AU	Australia	GA	Gabon	LV	Latvia	SZ	Swaziland
AZ	Azerbaijan	GB	United Kingdom	MC	Monaco	TD	Chad
BA	Bosnia and Herzegovina	GE	Georgia	MD	Republic of Moldova	TG	Togo
BB	Barbados	GH	Ghana	MG	Madagascar	TJ	Tajikistan
BE	Belgium	GN	Guinea	MK	The former Yugoslav Republic of Macedonia	TM	Turkmenistan
BF	Burkina Faso	GR	Greece			TR	Turkey
BG	Bulgaria	HU	Hungary	ML	Mali	TT	Trinidad and Tobago
BJ	Benin	IE	Ireland	MN	Mongolia	UA	Ukraine
BR	Brazil	IL	Israel	MR	Mauritania	UG	Uganda
BY	Belarus	IS	Iceland	MW	Malawi	US	United States of America
CA	Canada	IT	Italy	MX	Mexico	UZ	Uzbekistan
CF	Central African Republic	JP	Japan	NE	Niger	VN	Viet Nam
CG	Congo	KE	Kenya	NL	Netherlands	YU	Yugoslavia
CH	Switzerland	KG	Kyrgyzstan	NO	Norway	ZW	Zimbabwe
CI	Côte d'Ivoire	KP	Democratic People's Republic of Korea	NZ	New Zealand		
CM	Cameroon			PL	Poland		
CN	China	KR	Republic of Korea	PT	Portugal		
CU	Cuba	KZ	Kazakstan	RO	Romania		
CZ	Czech Republic	LC	Saint Lucia	RU	Russian Federation		
DE	Germany	LI	Liechtenstein	SD	Sudan		
DK	Denmark	LK	Sri Lanka	SE	Sweden		
EE	Estonia	LR	Liberia	SG	Singapore		

METHOD FOR THE SEPARATE AUTHENTICATION OF A TEMPLATE AND USER DATA

FIELD OF THE INVENTION

The present invention relates to the secure handling of data and more particularly concerns a method for separately authenticating a template and user data inserted in the template.

BACKGROUND OF THE INVENTION

There are many computer systems that have been designed to create, store, approve, revise or verify data electronically. Many of the documents that have been created through these systems have relied on a pre-existing template as a means of assembling data. This facilitates the means of data entry and allows the user to store the data and the template on one document. The use of the template also contributes to a less time-consuming process of entering information on an electronic document, a process that may contribute to fewer costs than those associated with paper-based data collection.

While there exist a great number of systems that may facilitate the creation, serial approval, storage and authentication of documents or of templates, there is no known system to date that can enable users to separate user data from template information. Current systems allow users to create templates and enter data in them. The data therefore becomes bound to the template in a single document. However, such systems do not have the capacity to enable users to securely approve, store and authenticate each portion separately, to approve multiple templates or, alternatively, opt to recreate the complete document.

Existing systems vary in the scope of the functions they can perform. Some are particularly limited, such as U.S. patent no. 4,933,969 to

Marshall et al., which primarily addresses authentication and storage. This mechanism stores information and protects against unauthorized modifications. While this type of data authentication system contributes greatly to ensuring the security and integrity of data, it lacks the capacity for the generation, approval and secure storage of both template information and user data.

Other systems offer certain types of electronic functions that are related to the generation and authentication of electronic signatures. For example, U.S. patent no. 5,195,133 to Kapp et al. describes a system designed to generate a completed payment document, which can be signed by a customer, and then capture that customer's signature in digital form. The principal feature of this mechanism is that it seeks to ensure that a signature approving a particular document was, in fact, captured at the time of the completion of the transaction to which it relates and was not obtained on some other occasion and merely reproduced for the particular transaction in question. The Kapp et al. patent creates a digital record of the transaction and captures a digital representation of the signature at the time the transaction is completed. This system then uses this digital record to encrypt the digital representation of the signature. However, it does not offer any possibility of generating or approving a template document separately from the user data or the electronic approval.

Other technology provides for the creation of an electronic signature for a particular signer only, and cannot be used for any document other than the one for which the signature was given (U.S. patent no. 5,689,567). U.S. patent no. 5,606,609 to Houser and Adler is a system designed to verify the integrity or signer of electronic documents. This is accomplished by embedding and encrypting security information in the electronic document at a location selected by the signer. When the electronic document is subsequently displayed, the technology decrypts the security information and verifies the identity of the signer. In another mechanism,

another method operates to authenticate and verify users on a network (U.S. patent no. 5,706,427). The possible applications of any of the aforementioned systems, albeit useful for certain purposes, are nonetheless limited as they do not allow for the creation, approval or authentication of template information distinct from the user data.

While each of the aforementioned systems can be useful for electronic business processes, they all have certain deficiencies. These mechanisms lack the capacity to enable the user to generate, approve, store and authenticate template information separately from user data, with the possibility of subsequently merging the two later in a complete document. Current technology operates such that any user data entered on the template becomes bound to the template in one document. The present invention allows users to access either the template data, multiple templates and/or the user data as independent files. Moreover, the technology ensures that no unauthorized modifications can be made to either file or to the complete document. This therefore accords the user greater flexibility in accessing each file without compromising the security or authenticity of the data.

The Remote Template Approval ("RTA") can serve as a vital tool facilitating electronic business processes. Many industries, such as insurance for example, which rely on templates and standard forms as a means of gathering information or selling and marketing services can greatly benefit from this technology. The RTA would enable those marketing these services to securely store and access user data separately from the templates, while individual template information could be generated, accessed or modified for each subsequent user or purchaser. This would represent an efficient way of gathering, storing and authenticating client and template information. In addition, it would offer an easy and secure medium through which users or consumers could submit information and purchase services on-line.

Clearly then, as electronic business transactions become even more prevalent, the need to generate and store template information and user data as separate entities will become more pronounced as well. As this occurs, the need for the Remote Template Approval mechanism will expand with it.

SUMMARY OF THE INVENTION

The present invention provides a system and method designed to facilitate remote template approval. This system will enable users to separate user data from template information and authenticate and verify each portion separately. Thus, by virtue of this method, users will be able to approve template information separately from the data added to the template. Preferably, this invention will also enable users to securely recreate the complete document composed of both data and template and verify its authenticity. Such a process would represent a marked improvement over existing systems which enable users to add data to existing templates in such a fashion as to bind the data to the template in one document. The present invention allows the user to securely access the template and the data as distinct records, or to, optionally, access the complete document.

Accordingly, the present invention provides a method for the separate authentication of a template and of user data inserted therein, comprising the steps of:

a) providing the template, said template having a corresponding template ID and template Document Authentication Code, hereinafter referred to as DAC(t), linked thereto;

b) inserting the user data in the template;

c) extracting the user data from the template;

d) generating a user data Document Authentication Code, hereinafter referred to as DAC(d), based on the user data; and

e) storing the template ID, DAC(t), the user data and DAC(d) in an Approval Data Packet, hereinafter referred to as ADP.

There is also provided a method for the separate authentication of a template having entry fields and user data inserted into said fields, comprising the steps of:

a) selecting a template ID and a corresponding template Document Authentication Code, hereinafter referred to as DAC(t), linked to the template;

b) entering the user data;

c) linking the user data to the fields of the template;

d) generating a user data Document Authentication Code, hereinafter referred to as DAC(d), based on the user data; and

e) storing the template ID, DAC(t), the user data and DAC(d) in an Approval Data Packet, hereinafter referred to as ADP.

The present invention further provides a method for the separate authentication of a template and of user data inserted therein, comprising the steps of:

a) providing the template, said template having a corresponding template ID and template Document Authentication Code, hereinafter referred to as DAC(t), linked thereto;

b) inserting the user data in the template;

c) generating a complete document Document Authentication Code, hereinafter referred to as DAC(c), based on the template with the user data therein;

d) extracting the user data from the template;

e) generating a user data Document Authentication Code, hereinafter referred to as DAC(d), based on the user data; and

f) storing the template ID, DAC(t), the user data, DAC(c) and DAC(d) in an Approval Data Packet, hereinafter referred to as ADP.

Also provided is a method for the separate authentication of a template and of user data inserted therein by multiple users, comprising the steps of:

a) authenticating a template and user data from a first user according to the last method described above; and

b) for each subsequent user of the multiple users, performing the substeps of:

i) retrieving the template and DAC(c);

ii) inserting user data from previous users in the template;

iii)generating for the template with the user data from previous users therein a new complete document Document Authentication Code, hereinafter referred to as DAC(nc);

iv) comparing DAC(nc) with DAC(c), and proceeding only if DAC(nc) is equal to DAC(c);

v) inserting data from the current user in the template;

vi) generating a DAC(c), based on the template with the user data from the previous users and current user therein;

vii) extracting the user data from the previous users and current user from the template;

viii) generating a DAC(d), based on the user data extracted in step vii); and

ix) storing the user data, DAC(c) and DAC(d) in ADP.

The present invention can have numerous applications. For example, it could enable users to create and approve one document on one system (e-mail for example), with the target template indicated in the ADP, and send it to another system, which may be the same system or a completely different one. The message can then be entered into the actual template document with all the proper formatting and no need to convert the document.

This invention would be useful for many industries that rely on templates as a means of collecting data. The same template could be generated for each new user and the data collected could be stored separately or could also be combined with the template to create a completed document. This method would allow users to re-generate the template for each subsequent user.

The present invention and its advantages will be better understood upon reading the following non-restrictive description of embodiments thereof with reference to the accompanying drawings.

BRIEF DESCRIPTION OF THE DRAWINGS

FIG. 1 is a flow chart representing the main steps of a method for the separate authentication of a template and of user data inserted therein in accordance with a preferred embodiment of the present invention.

FIG. 2 is a flow chart detailing step f of the method of FIG. 1.

FIG. 3 is a flow chart representing the main steps of a method for the separate authentication of a template and of user data inserted therein in accordance with an alternative embodiment of the invention.

FIG. 4 is a flow chart representing the main steps of a method for the separate authentication of a template and of user data inserted therein in accordance with another embodiment of the invention.

FIG. 5 is a flow chart detailing step g of the method of FIG. 4.

FIG. 6 is a flow chart detailing another variant for step g of the method of FIG. 4.

FIG. 7 is a flow chart representing the main steps of a method for the separate authentication of a template and of user data inserted therein in accordance with yet another embodiment of the invention.

DESCRIPTION OF PREFERRED EMBODIMENTS OF THE INVENTION

Referring to FIGs. 1 and 2, the steps of a method for the separate authentication of a template and user data inserted in the template are shown. This method allows the secure handling of the template and user data independently, without having to store the user data inside the template.

The first step a) of the method of FIG. 1 consists of providing the template itself. A template ID, identifying the particular template chosen, and a template Document Authentication code, DAC(t), are both linked to the template. DAC(t) is a code characterizing precisely the template's content, and is preferably generated through a one-way hash function. If the template is not pre-existing, step a) may include the substep of generating the template, creating the template ID and DAC(t) and storing the last two in an appropriate location, which can for example be inside the template itself or in a linked storage system.

The second step b) consists of inserting the user data in the template. The term "user data" is understood as encompassing any relevant information that may be entered in a template, including a user signature and the date of signing. The method may therefore be used in the context of the remote approval of a document. The template preferably has specific fields where the user data may be received.

The user data is then extracted from the template in accordance with step c), and in the next step d) a user data Authentication Code (DAC(c)) is generated, based on the user data itself independently of the template.

Step e) consists of storing the template ID, DAC(t), the user data and DAC(c) in an Approval Data Packet (ADP) which may be encrypted for security. The user data may alternatively be stored elsewhere and a link to its location may be provided in the ADP.

Referring to FIGS. 1 and 2, there is shown an optional step f) of reconstructing a complete document including both the template and the

user data. In accordance with this additional step, the template ID and DAC(t) are first retrieved from the ADP, and the template corresponding to the template ID is accessed and opened. A new DAC (DAC(nt)) is generated on the opened template, and compared to DAC(t). Corrective action is to be taken if they don't match. If they do match, the user data and DAC(d) are also retrieved. A DAC(nd) is generated on the user data and compared to DAC(d). If they also match, the user data may then be inserted in the template.

In an alternate embodiment of the invention, illustrated in FIG. 3, the method described above may be performed without actually accessing the template. In this embodiment, a template ID and the corresponding DAC(t) are selected, and the user data is entered, preferably in answer to prompts for particular information. The user data entered is then linked to corresponding fields in the template, so that a complete document including both the template and the user data may later be reconstructed.

Referring to FIGs. 4, 5 and 6, there is shown yet another embodiment of the invention. In this particular embodiment, a step is added between steps b) and c) of FIG. 1 where a DAC(c) is generated based on the template with the user data therein, before the user data is extracted from the template. This DAC(c) is stored in the ADP with the other relevant information. In this manner, when reconstructing the complete document, additional substeps of generating a DAC(nc) on the complete document once the user data is inserted in the template and comparing this DAC(nc) with DAC(c) may be performed, as shown in FIG. 5. Alternatively, only the DACs of the complete documents may be compared, completely bypassing the verifications of the separate template and user data, as illustrated in FIG. 6.

Referring to FIG. 7, there is shown another embodiment of the invention where multiple users insert user data sequentially in a single template. The method includes the steps of:

a) authenticating a template and user data from a first user according to the method of FIG. 4. In this manner, an ADP is created containing the template ID, DAC(t), the user data, DAC(d) and DAC(c).

b) for each subsequent user of the multiple users, the following substeps are performed:

i) retrieving the template and DAC(c) from the ADP;

ii) inserting user data from previous users in the template. The document thereby generated corresponds to the complete document of the previous iteration;

iii) generating for the template with the user data from previous users therein a new complete document Document Authentication Code (DAC(nc));

iv) comparing DAC(nc) with DAC(c), and proceeding only if DAC(nc) is equal to DAC(c);

v) inserting data from the current user in the template;

vi) generating a DAC(c), based on the template with the user data from the previous users and current user therein;

vii) extracting the user data from the previous users and current user from the template;

viii) generating a DAC(d), based on the user data extracted in step vii); and

ix) storing the user data, DAC(c) and DAC(d) in ADP. DAC(c) and DAC(d) thereby replace the previously stored values of these variables.

An additional step of reconstructing the complete document, which in this case corresponds to the document generated in the last iteration of step b), may also be performed, either in the manner illustrated in FIG. 5 or FIG. 6.

Of course, numerous changes could be made to the preferred embodiment disclosed hereinabove without departing from the scope of the invention as defined in the appended claims.

WHAT IS CLAIMED IS:

1. A method for the separate authentication of a template and of user data inserted therein, comprising the steps of:

a) providing the template, said template having a corresponding template ID and template Document Authentication Code, hereinafter referred to as DAC(t), linked thereto;

b) inserting the user data in the template;

c) extracting the user data from the template;

d) generating a user data Document Authentication Code, hereinafter referred to as DAC(d), based on the user data; and

e) storing the template ID, DAC(t), the user data and DAC(d) in an Approval Data Packet, hereinafter referred to as ADP.

2. The method according to claim 1, wherein step a) comprises the substeps of:

i) generating the template;

ii) creating the template ID;

iii) creating DAC(t); and

iv) storing the template ID and DAC(t) in a location linked to the template.

3. The method according to claim 2, wherein substep a)iii) comprises generating DAC(t) from a one-way hash function.

4. The method according to claim 2, wherein, in substep a) iv), the location linked to the template is inside said template.

5. The method according to claim 2, wherein, in substep a) iv), the location linked to the template is a linked storage system.

6. The method according to claim 1, wherein step e) further comprises encrypting the ADP.

7. The method according to claim 1, further comprising an additional step f) of reconstructing an authenticated complete document, said complete document including the template and the user data.

8. The method according to claim 7, wherein step f) comprises the substeps of:

i) retrieving the template ID and DAC(t) from the ADP;

ii) opening the template corresponding to said template ID;

iii) generating for said template a new template Document Authentication Code, hereinafter referred to as DAC(nt);

iv) comparing DAC(nt) with DAC(t), and proceeding only if DAC(nt) is equal to DAC(t);

v) retrieving the user data and DAC(d) from the ADP;

vi) generating for said user data a new user data Document Authentication Code, hereinafter referred to as DAC(nd);

vii) comparing DAC(nd) with DAC(d), and proceeding only if DAC(nd) is equal to DAC(d); and

viii) inserting the user data in the template.

9. A method for the separate authentication of a template having entry fields and user data inserted into said fields, comprising the steps of:

a) selecting a template ID and a corresponding template Document Authentication Code, hereinafter referred to as DAC(t), linked to the template;

b) entering the user data;

c) linking the user data to the fields of the template;

d) generating a user data Document Authentication Code, hereinafter referred to as DAC(d), based on the user data; and

e) storing the template ID, DAC(t), the user data and DAC(d) in an Approval Data Packet, hereinafter referred to as ADP.

10. The method according to claim 9, wherein step b) further comprises prompting the user for the user data.

11. The method according to claim 9, wherein step e) further comprises encrypting the ADP.

12. The method according to claim 9, further comprising an additional step f) of reconstructing an authenticated complete document, said complete document including the template and the user data.

13. The method according to claim 12, wherein step f) comprises the substeps of:

i) retrieving the template ID and DAC(t) from the ADP;

ii) opening the template corresponding to said template ID;

iii) generating for said template a new template Document Authentication Code, hereinafter referred to as DAC(nt);

iv) comparing DAC(nt) with DAC(t), and proceeding only if DAC(nt) is equal to DAC(t);

v) retrieving the user data and DAC(d) from the ADP;

vi) generating for said user data a new user data Document Authentication Code, hereinafter referred to as DAC(nd);

vii) comparing DAC(nd) with DAC(d), and proceeding only if DAC(nd) is equal to DAC(d); and

viii) inserting the user data in the template.

14. A method for the separate authentication of a template and of user data inserted therein, comprising the steps of:

a) providing the template, said template having a corresponding template ID and template Document Authentication Code, hereinafter referred to as DAC(t), linked thereto;

b) inserting the user data in the template;

c) generating a complete document Document Authentication Code, hereinafter referred to as DAC(c), based on the template with the user data therein;

d) extracting the user data from the template;

e) generating a user data Document Authentication Code, hereinafter referred to as DAC(d), based on the user data; and

f) storing the template ID, DAC(t), the user data, DAC(c) and DAC(d) in an Approval Data Packet, hereinafter referred to as ADP.

15. The method according to claim 14, wherein step a) comprises the substeps of:

i) generating the template;

ii) creating the template ID;

iii) creating DAC(t); and

iv) storing the template ID and DAC(t) in a location linked to the template.

16. The method according to claim 15, wherein substep a)iii) comprises generating DAC(t) from a one-way hash function.

17. The method according to claim 15, wherein, in substep a) iv), the location linked to the template is inside said template.

18. The method according to claim 15, wherein, in substep a) iv), the location linked to the template is a linked storage system.

19. The method according to claim 14, wherein step f) further comprises encrypting the ADP.

20. The method according to claim 14, further comprising an additional step g) of reconstructing an authenticated complete document, said complete document including the template and the user data.

21. The method according to claim 20, wherein step g) comprises the substeps of:

i) retrieving the template ID, DAC(t) and DAC(c) from the ADP;

ii) opening the template corresponding to said template ID;

iii) generating for said template a new template Document Authentication Code, hereinafter referred to as DAC(nt);

iv) comparing DAC(nt) with DAC(t), and proceeding only if DAC(nt) is equal to DAC(t);

v) retrieving the user data and DAC(d) from the ADP;

vi) generating for said user data a new user data Document Authentication Code, hereinafter referred to as DAC(nd);

vii) comparing DAC(nd) with DAC(d), and proceeding only if DAC(nd) is equal to DAC(d);

viii) inserting the user data in the template;

ix) generating for the template with the user data therein a new complete document Document Authentication Code, hereinafter referred to as DAC(nc); and

x) comparing DAC(nc) with DAC(c), and proceeding only if DAC(nc) is equal to DAC(c).

22. The method according to claim 20, wherein step g) comprises the substeps of:

i) retrieving the template ID, the user data and DAC(c) from the ADP;

ii) opening the template corresponding to said template ID;

iii) inserting the user data in the template;

iv) generating for the template with the user data therein a new complete document Document Authentication Code, hereinafter referred to as DAC(nc); and

v) comparing DAC(nc) with DAC(c), and proceeding only if DAC(nc) is equal to DAC(c).

23. A method for the separate authentication of a template and of user data inserted therein by multiple users, comprising the steps of:

a) authenticating a template and user data from a first user according to the method of claim 14; and

b) for each subsequent user of the multiple users, performing the substeps of:

i) retrieving the template and DAC(c);

ii) inserting user data from previous users in the template;

iii)generating for the template with the user data from previous users therein a new complete document Document Authentication Code, hereinafter referred to as DAC(nc);

iv) comparing DAC(nc) with DAC(c), and proceeding only if DAC(nc) is equal to DAC(c);

v) inserting data from the current user in the template;

vi) generating a DAC(c), based on the template with the user data from the previous users and current user therein;

vii) extracting the user data from the previous users and current user from the template;

viii) generating a DAC(d), based on the user data extracted in step vii); and

ix) storing the user data, DAC(c) and DAC(d) in ADP.

24. The method according to claim 23, further comprising an additional step c) of reconstructing an authenticated complete document, said complete document including the template and the user data from all of the multiple users.

25. The method according to claim 24, wherein step c) comprises the substeps of:

i) retrieving the template ID, DAC(t) and DAC(c) from the ADP;

ii) opening the template corresponding to said template ID;

iii) generating for said template a new template Document Authentication Code, hereinafter referred to as DAC(nt);

iv) comparing DAC(nt) with DAC(t), and proceeding only if DAC(nt) is equal to DAC(t);

v) retrieving the user data and DAC(d) from the ADP;

vi) generating for said user data a new user data Document Authentication Code, hereinafter referred to as DAC(nd);

vii) comparing DAC(nd) with DAC(d), and proceeding only if DAC(nd) is equal to DAC(d);

viii) inserting the user data in the template;

ix) generating for the template with the user data therein a new complete document Document Authentication Code, hereinafter referred to as DAC(nc); and

x) comparing DAC(nc) with DAC(c), and proceeding only if DAC(nc) is equal to DAC(c).

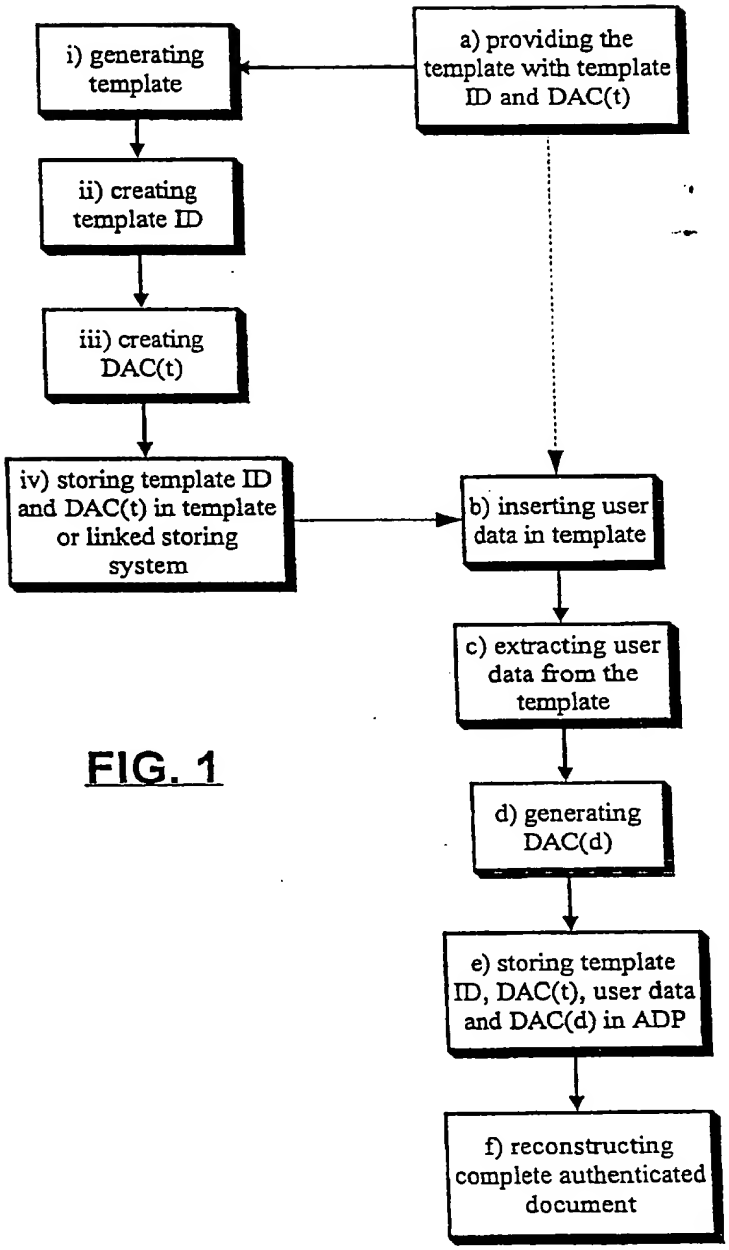

a) providing the template with template ID and DAC(t)
i) generating template
ii) creating template ID
iii) creating DAC(t)
iv) storing template ID and DAC(t) in template or linked storing system
b) inserting user data in template
c) extracting user data from the template
d) generating DAC(d)
e) storing template ID, DAC(t), user data and DAC(d) in ADP
f) reconstructing complete authenticated document

FIG. 1

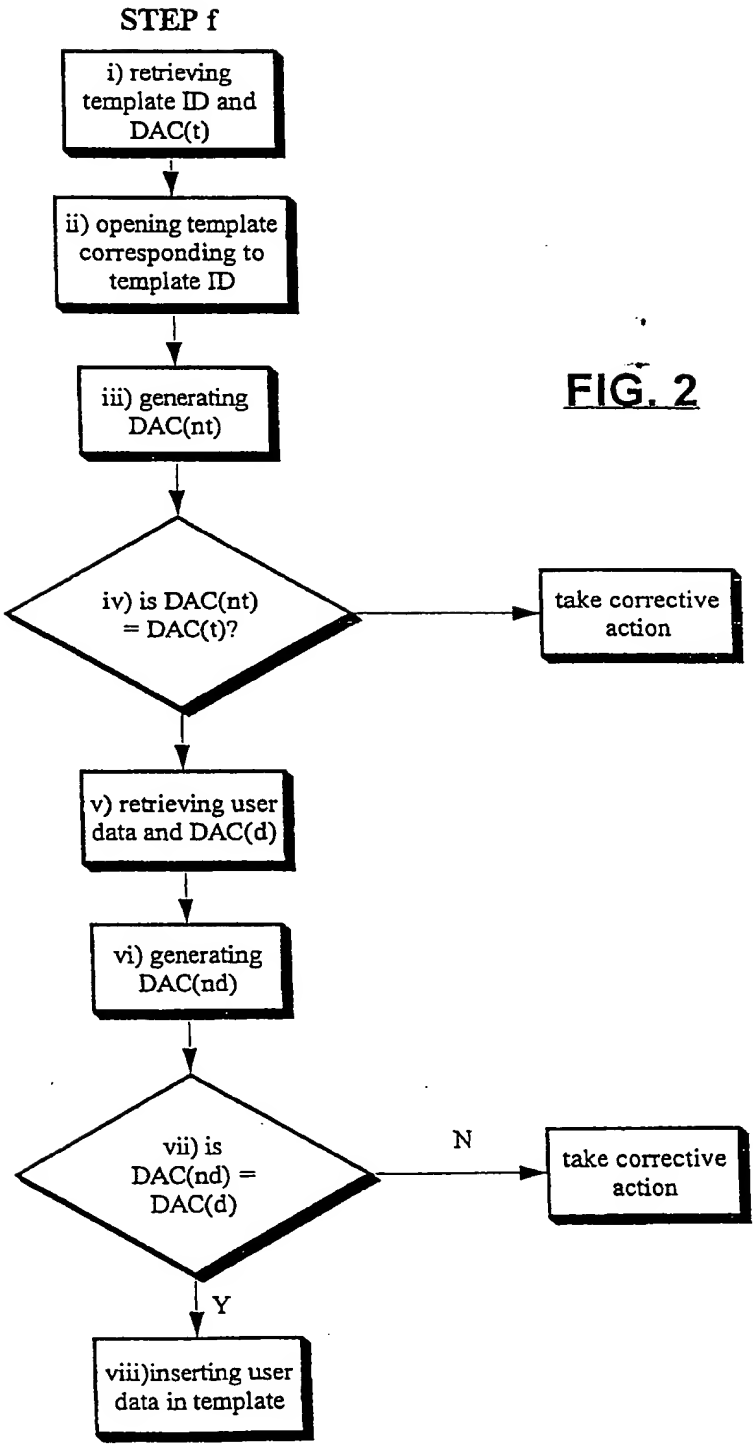

STEP f
i) retrieving template ID and DAC(t)
ii) opening template corresponding to template ID
iii) generating DAC(nt)
iv) is DAC(nt) = DAC(t)?
take corrective action
v) retrieving user data and DAC(d)
vi) generating DAC(nd)
vii) is DAC(nd) = DAC(d)
N
take corrective action
Y
viii)inserting user data in template

FIG. 2

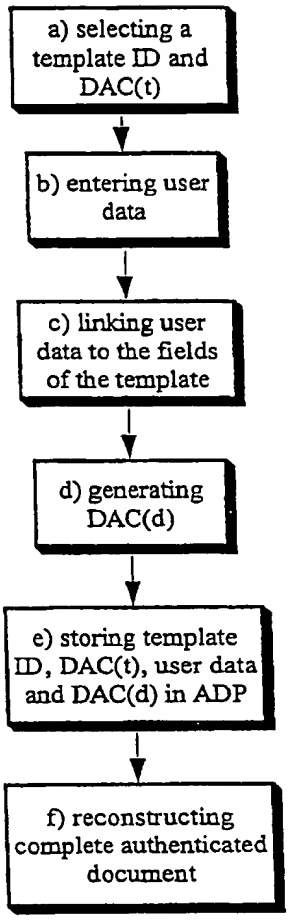

a) selecting a template ID and DAC(t)
b) entering user data
c) linking user data to the fields of the template
d) generating DAC(d)
e) storing template ID, DAC(t), user data and DAC(d) in ADP
f) reconstructing complete authenticated document

FIG. 3

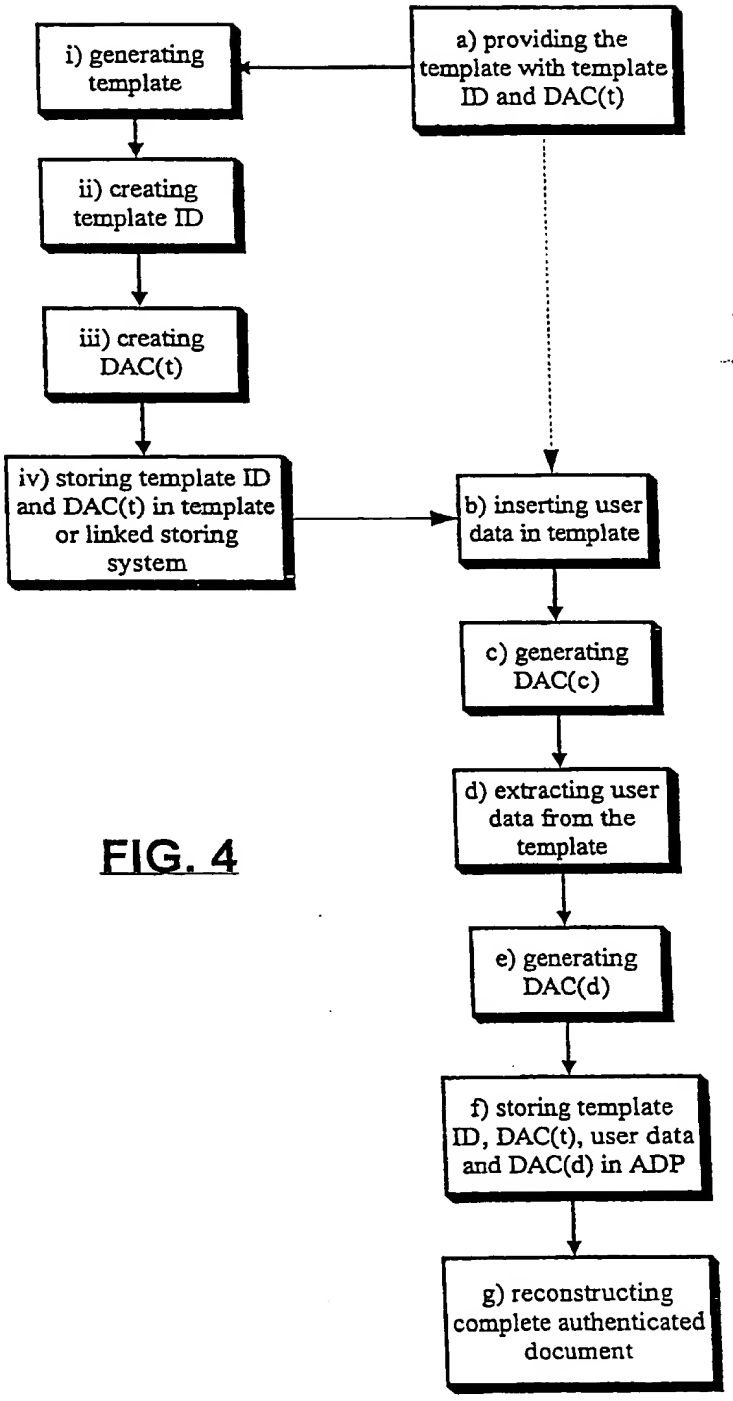

a) providing the template with template ID and DAC(t)
i) generating template
ii) creating template ID
iii) creating DAC(t)
iv) storing template ID and DAC(t) in template or linked storing system
b) inserting user data in template
c) generating DAC(c)
d) extracting user data from the template
e) generating DAC(d)
f) storing template ID, DAC(t), user data and DAC(d) in ADP
g) reconstructing complete authenticated document

FIG. 4

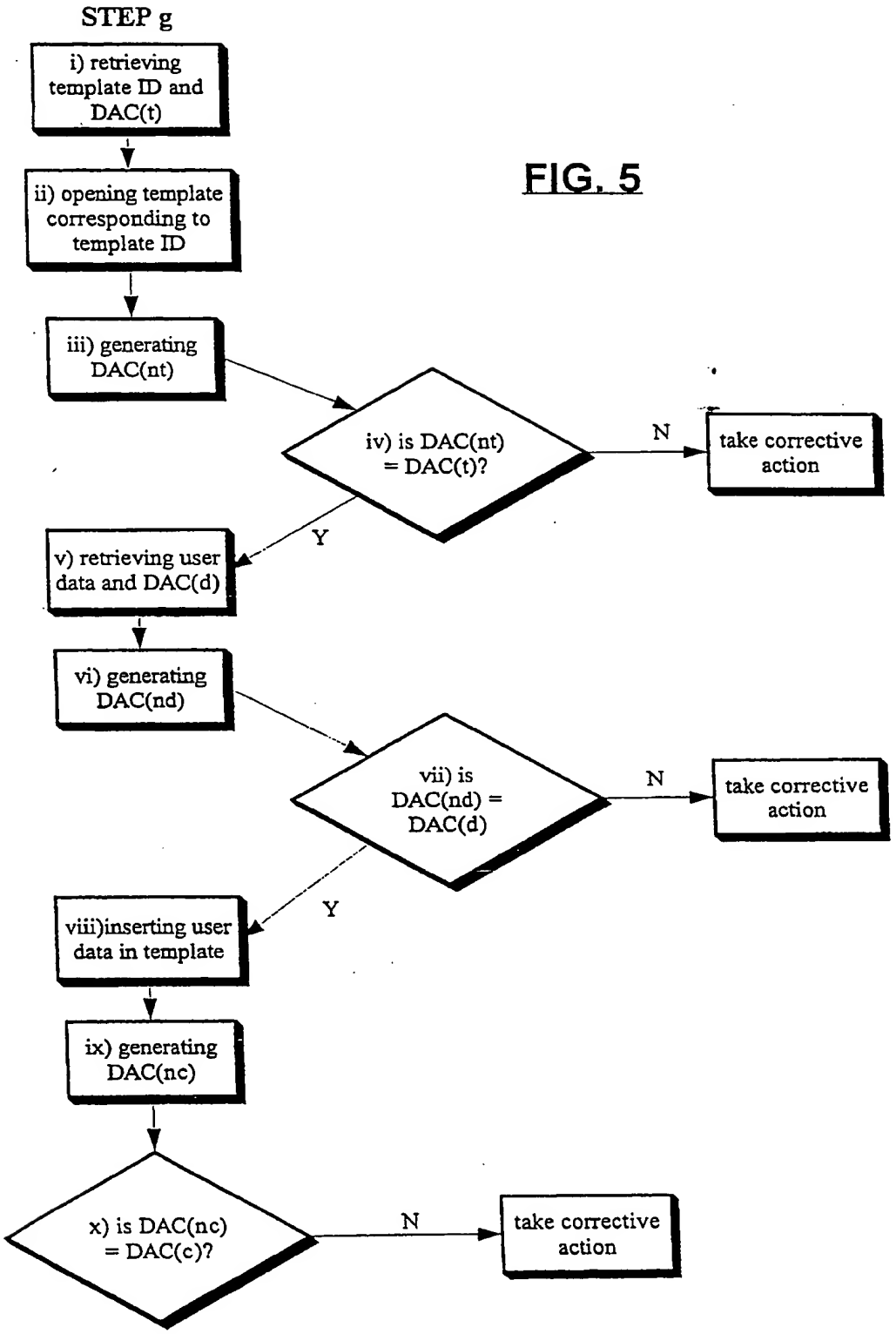

STEP g
i) retrieving template ID and DAC(t)
ii) opening template corresponding to template ID
iii) generating DAC(nt)
iv) is DAC(nt) = DAC(t)?
N
take corrective action
Y
v) retrieving user data and DAC(d)
vi) generating DAC(nd)
vii) is DAC(nd) = DAC(d)
N
take corrective action
Y
viii)inserting user data in template
ix) generating DAC(nc)
x) is DAC(nc) = DAC(c)?
N
take corrective action

FIG. 5

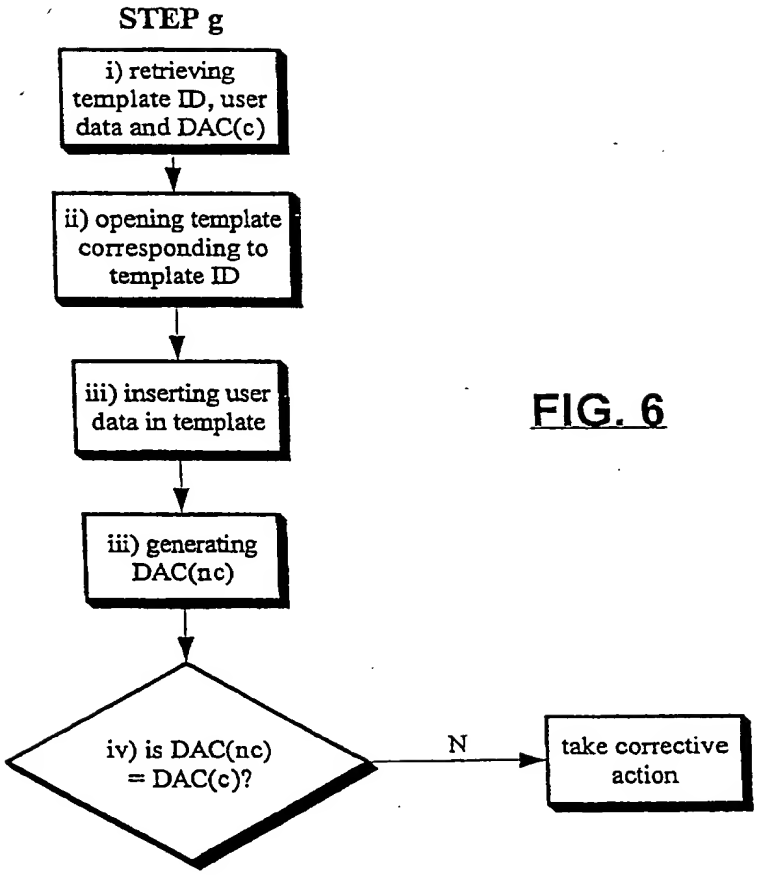

STEP g
i) retrieving template ID, user data and DAC(c)
ii) opening template corresponding to template ID
iii) inserting user data in template
iii) generating DAC(nc)
iv) is DAC(nc) = DAC(c)?
N
take corrective action

FIG. 6

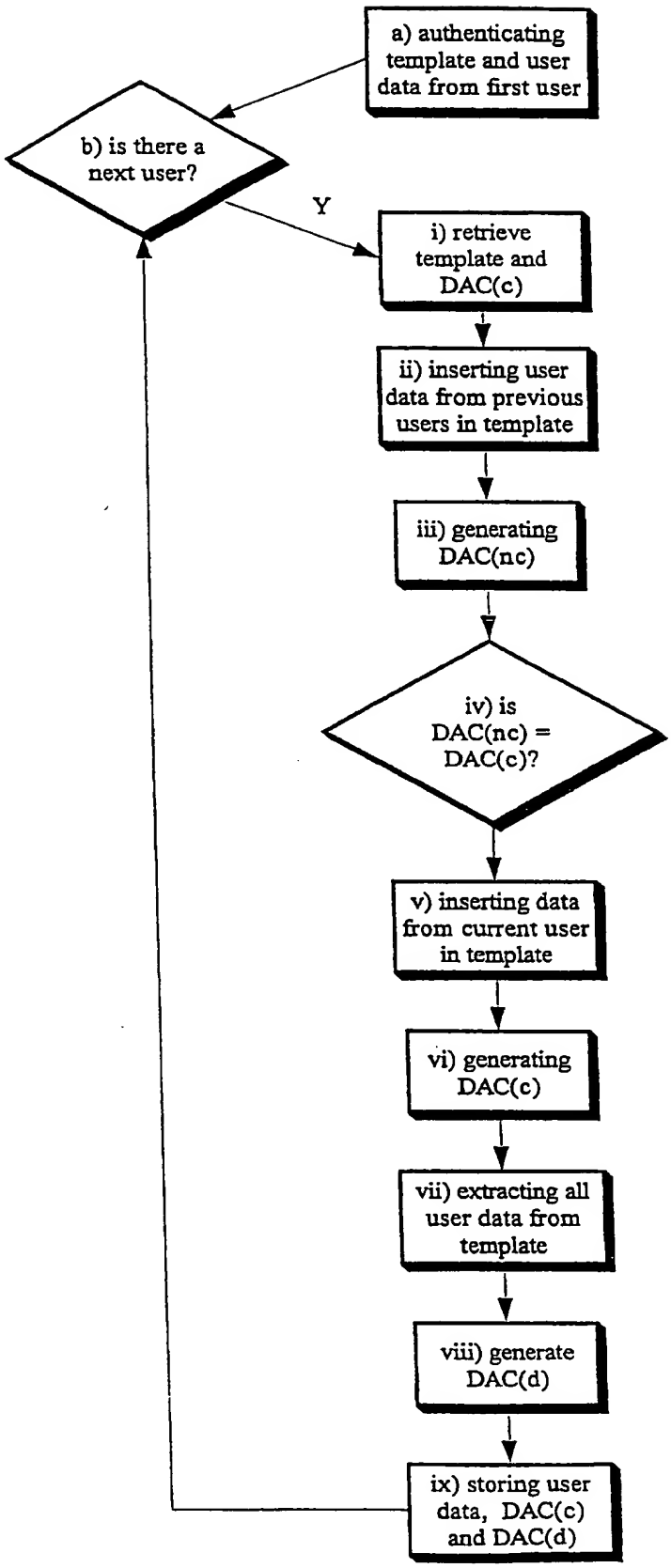

a) authenticating template and user data from first user
b) is there a next user?
Y
i) retrieve template and DAC(c)
ii) inserting user data from previous users in template
iii) generating DAC(nc)
iv) is DAC(nc) = DAC(c)?
v) inserting data from current user in template
vi) generating DAC(c)
vii) extracting all user data from template
viii) generate DAC(d)
ix) storing user data, DAC(c) and DAC(d)

FIG. 7

INTERNATIONAL SEARCH REPORT

Interr ...al Application No
PCT/CA 99/00891

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 G06F1/00

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 7 G06F H04L

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	EP 0 565 314 A (FISHER ADDISON) 13 October 1993 (1993-10-13) page 2, line 9 -page 10, line 37; figures 1-11,21,22	1,9,14
A	WO 98 03927 A (O'NEIL) 29 January 1998 (1998-01-29) page 1, line 1 -page 4, line 13 page 6, line 29 -page 19, line 32; figures 4,15	1,9,14
A	THE IMPACT OF TECHNOLOGY ON THE NOTARY PROCESS, 'Online! 10 February 1998 (1998-02-10), XP002125327 Retrieved from the Internet: <URL:law.uark.edu/[gahlers/notary.htm> 'retrieved on 1999-12-10! the whole document	1,9,14

[ ] Further documents are listed in the continuation of box C.

[X] Patent family members are listed in annex.

* Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
15 December 1999	28/12/1999

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Soler, J

2

Form PCT/ISA/210 (second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

Information on patent family members

Interr nal Application No
PCT/CA 99/00891

Patent document cited in search report	Publication date	Patent family member(s)	Publication dat
EP 565314 A	13-10-1993	AU 3560793 A	07-10-1993
		CA 2093094 A	07-10-1993
		JP 6295286 A	21-10-1994
		US 5390247 A	14-02-1995
		US 5337360 A	09-08-1994
WO 9803927 A	29-01-1998	EP 0912954 A	06-05-1999

INTERNATIONAL SEARCH REPORT

Interr ·al Application No
PCT/CA 99/00891

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 G06F1/00

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 7 G06F H04L

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	EP 0 565 314 A (FISHER ADDISON) 13 October 1993 (1993-10-13) page 2, line 9 -page 10, line 37; figures 1-11,21,22	1,9,14
A	WO 98 03927 A (O'NEIL) 29 January 1998 (1998-01-29) page 1, line 1 -page 4, line 13 page 6, line 29 -page 19, line 32; figures 4,15	1,9,14
A	THE IMPACT OF TECHNOLOGY ON THE NOTARY PROCESS, 'Online! 10 February 1998 (1998-02-10), XP002125327 Retrieved from the Internet: <URL:law.uark.edu/jgahlers/notary.htm> 'retrieved on 1999-12-10! the whole document	1,9,14

[ ] Further documents are listed in the continuation of box C.

[X] Patent family members are listed in annex.

° Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
15 December 1999	28/12/1999

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Soler, J

2

Form PCT/ISA/210 (second sheet) (July 1992)